REMARKS

New claim 63 has been added. Claims 23-63 are presently pending. No new matter has been added. The new claim is supported by the original disclosure. In view of the foregoing amendments and the following remarks, the Applicant respectfully submit that all of the presently pending claims are allowable. Reconsideration of the Application is respectfully requested.

1. Rejection of claims 23-30, 32-48 and 50-62 (35 U.S.C. § 103(a))

Claims 23-30, 32-48 and 50-62 are rejected under 35 U.S.C. § 103(a), the Examiner contending they are obvious over Alcorn et al. U.S. Patent No. 6,149,522 ("Alcorn") in view of Hansmann et al. U.S. Patent No. 6,892,301 ("Hansmann"). Applicant notes that the third paragraph on page 3 of the Office action refers to an '892 reference. Applicant respectfully notes that there is no cited '892 reference.

The Applicant notes that while the Office Action includes claims 61 and 62 in this rejection, the claims are not discussed in this section. Rather, claims 61 and 62 are discussed in a subsequent section. For purposes of this response, it is assumed claims 61 and 62 should be discussed in the subsequent section. Clarification is requested.

To establish a prima facie case of obviousness under 35 U.S.C. § 103(a), the prior art references must teach or suggest all the claim limitations. M.P.E.P. § 2143.03. Applicant respectfully submits that neither Alcorn nor Hansmann, alone or combination, teach or suggest all the limitations of the rejected claims.

Alcorn generally describes a method of authenticating game data sets in a casino gaming terminal. Authentication generates a computer message digest of a data set through a hash function, which is later compared by a receiver to ensure the data set has not been modified in transit. The purpose of authentication is to detect any tampering that may have occurred on the game data sets. Game data sets are stored in unrestricted storage. A separate, unalterable ROM contains authentication software for calculating a signature from the stored game data sets using a hash function. Alcorn does not teach or suggest downloading of security keys with game data sets.

Hansmann generally describes a mechanism for securely reading information from chipcards.

Claim 43 recites, in relevant part, "receiving at the gaming terminal a second non-resident security key separately from a first resident security key and the second encrypted electronic information." The Office Action acknowledges that this feature is not taught or suggested by the cited Alcorn reference. It is believed, that the Office Action intends to propose that Alcorn be modified in light of Hansmann to provide this feature, although as noted above, an '892 patent is cited. Applicant respectfully submits that this is an improper hindsight reconstruction. The Office Action contends that it would have been obvious "to include a means to encrypt and decrypt of the game operation code with addition secret keys provided at the time of download." The Office Action further contends that "One of ordinary skill in the art would have been motivated to perform such a modification to support modifications to terminal devices that have a missing software component." Restated, the Office Action contends that Hansmann teaches adding the chipcard to provide a key for downloading content in Alcorn. However, Hansmann has no such teaching – the purpose of the chipcard in Hansmann is not to unlock content downloading, rather programs are downloaded in Hansmann to enable reading the chipcard, an entirely different type of process.

An ordinary artisan would not be lead to apply Hansmann's special purpose chipcard reader enablement technique to the different field of game software downloading for game terminals. Hansmann's terminal device is not any terminal device, let alone a game terminal device, but rather is a chip card reader that is unable to read a particular chipcard. Hansmann does not address game terminals, gaming software, or even general purpose terminals or software, but rather focuses entirely on the particular problems associated with chipcard readers. In contrast, Applicant's claimed invention is specifically directed to a method for securely downloading information to a gaming terminal. The cited Alcorn reference also directly addresses a gaming application.

The cited portion of Hansmann reference deals specifically with a what Hansmann calls a terminal device – "a chip card reader" that "cannot access a chip card or fulfill a particular function of a chip card". *See* Hansmann 3:63-66. Essentially, Hansmann's terminal device is a chipcard processor, e.g., a chipcard reader. Hansmann is directed to the problem of a chipcard reader which receives a chipcard that it is unable to process – the chipcard reader then needs to receive additional functionality to allow it to process input from the chipcard input device. Hansmann does not address or suggesting addressing the problem of downloading new applications to game terminals. Hansmann's chipcard is not used as a key to enable or unlock the downloading of new gaming applications to a game terminal; and Hansmann does not suggest that this feature should be added to Alcorn. In Hansmann, the goal is reading the chipcard, not using the chipcard to enable downloading a new application. If anything, the proposed combination/modification would entirely invert the method of operation of Hansmann, where new software is downloaded to enable a chip card to be processed, not the other way around. If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *See* MPEP 2243.01 (*citing In re Ratti*, 270 F.2d 810 (CCPA 1959)).

Moreover, claim 43 also recites "decrypting the second encrypted electronic information into a second decrypted electronic information at the gaming terminal with at least the first resident security key and the second non-resident security key". Again the Office Action states that an ordinary artisan would be motivated to graft this feature from Hansmann to Alcorn "to support modifications to terminal devices that have a missing software component", citing Hansmann at 3:61. But a careful examination of this section of Hansmann shows this entire section deals with reading unreadable chip cards, i.e. to enable reading of new types of chipcards. The goal in Hansmann is to read new types of chipcards, not download new applications. Grafting this feature on to Alcorn, as discussed above, entirely inverts the purpose and method of operation of Hansmann's system.

Claims 44-48 and 50-60 depend from claim 43 and thus allowable over Alcorn in view of Hansmann for at least the same reasons as claim 43.

Separately and independently of the argument given above, claim 48 recites, in relevant part, "wherein the transmitting is accomplished with a physical electronic key removably attached to the gaming terminal." Col. 10, lines 28-33 of Alcorn, cited in the Office Action, generally describes a ROM 54 kept on file in a secure location to be compared against a ROM removed from a gaming machine. Thus, the ROM 54 does not transmit the second encrypted electronic information, but is used for storage purposes. Nor is the ROM 54 a physical electronic key removably attached to the gaming terminal because it is stored in a secure location and not at the gaming terminal. Thus, the cited references do not have the recited features of claim 48 and the rejection should be withdrawn.

Separately and independently of the argument given above, claim 50 recites, in relevant part, "determining a version information of the second encrypted electronic information with an information in the second non-resident security key." Col. 12, lines 52-62 and col. 9, lines 17-40 of Alcorn, cited in the Office Action, generally describes decrypting two signatures and validating data with the decrypted signatures. Neither of the two signatures, which are decrypted by the game terminal, comprises version information. Thus, the cited do not have the recited features of claim 50 and the rejection should be withdrawn.

Separately and independently of the argument given above, claim 52 recites, in relevant part, "the second decrypted information comprises game application code." Col. 12, lines 52-62 of Alcorn, cited in the Office Action, generally describes determining whether a game data set or game-modifying data set is valid, and if so, loading the new game data set or game modifying data set. A signature is decrypted as part of the validation process. The cited references do not suggest that either of the two signatures, which are decrypted, comprises game application code. No encrypted or decrypted game application code appears to be described. Thus, the cited references do not have the recited feature of claim 52 and the rejection should be withdrawn.

Separately and independently of the argument given above, claim 53 recites, in relevant part, "the second decrypted information comprises game system modules." Col. 12, lines 52-62 of Alcorn, cited in the Office Action, generally describes determining whether a game data set or game-modifying data set is valid, and if so, loading the new game data set or game modifying data set. A signature is decrypted as part of the validation process. The cited references do not describe that either of the two signatures, which are decrypted, comprises game system modules. No encrypted or decrypted game system modules appear to be described. Thus, the cited references do not have the recited feature of claim 53 and the rejection should be withdrawn.

Separately and independently of the argument given above, claim 54 recites, in relevant part, "the second decrypted information comprises game graphics and audio files." Col. 7, line 65 through col. 8, line 14 of Alcorn, cited in the Office Action, generally describes ROMs 29 and 30. The ROMs contain a system initialization code, an authentication program, an initial portion of the loader programs, game image and sound data, rules of game play and the like, and the signature associated with each particular casino game. The cited references do not describe that the signature, which is encrypted, comprises game graphics and audio files. The game image and sound data described by Alcorn is not encrypted or decrypted, thus they cannot be the claimed second decrypted information. Thus, the cited references fails to make obvious claim 54 and the rejection should be withdrawn.

Separately and independently of the argument given above, claim 55 recites, in relevant part, "the second decrypted information comprises new release game software files." Col. 12, lines 52-62 of Alcorn, cited in the Office Action, generally describes determining whether a game data set or game-modifying data set is valid, and if so, loading the new game data set or game modifying data set. A signature is decrypted as part of the validation process. Alcorn does not describe that either of the two signatures, which are decrypted, comprises new release game software files. Thus, the cited references fails to make obvious claim 55 and the rejection should be withdrawn.

Separately and independently of the argument given above, claim 56 recites receiving a third non-resident security key with the second encrypted electronic information at the gaming terminal. And also recites decrypting the third encrypted electronic information with the third key. A key received with a payload of information (i.e. the third key received with the second information) is then used to decrypt a *later* payload (i.e. the third information) of information. Embodiments covered by this feature include systems where updates to the system also update the keys which used to enable future updates. This feature is not described or taught by any of the cited references.

Separately and independently of the argument given above, claim 57 recites, in relevant part, "packaging the third non-resident security key and the second encrypted electronic information into one file." Col. 4, lines 43-67 of Alcorn, cited in the Office Action, generally describe a program or fixed data set preparation phase, wherein a first abbreviated bit string is computed and encrypted to provide an encrypted signature of the program. The cited references fail to describe, nor even suggest, packaging a security key together with an encrypted information into one file. Moreover, claim 57 depends from claim 56, and reading the two claims together specifically claims the feature where a key is transmitted with one set of downloaded information, and then used to decrypt a later-received set of downloaded information. Thus, the cited references fails to make obvious claim 57 and the rejection should be withdrawn.

Similar to claim 43, claim 23 recites, in relevant part, "a second non-resident security key residing outside the gaming terminal and received by the gaming terminal separately from the first resident security key and the second encrypted electronic information" and "the second decrypted electronic information decrypted from the second encrypted electronic information ... with at least the first resident security key and the second non-resident security key". The combination of Hansmann and Alcorn does not render this claim obvious for reasons similar to those given above for claim 43.

Claims 24-30 and 32-42 depend from claim 23 and thus should be patentable over the cited references for at least the same reasons as claim 23.

In addition, claim 29 recites, in relevant part, "a removable storage media removably attached to the gaming terminal, the removable storage media configured to receive and to transmit electronic information." Similar to the discussion of claim 48, the cited references do not teach or suggest this feature.

In addition, claim 30 recites, in relevant part, "a removable storage media removably attached to the gaming terminal, the removable storage media configured as a non-network connection." Similar to the discussion of claim 48, the cited references do not teach or suggest this feature.

In addition, claim 32 recites, in relevant part, "the second non-resident security key comprises information to determine a version information of the second encrypted electronic information." Similar to the discussion of claim 50, the cited references do not teach or suggest this feature.

In addition, claim 34 recites, in relevant part, "the second decrypted information comprises game application code." Similar to the discussion of claim 52, the cited references do not teach or suggest this feature.

In addition, claim 35 recites, in relevant part, "the second decrypted information comprises game system modules." Similar to the discussion of claim 53, the cited references do not teach or suggest this feature.

In addition, claim 36 recites, in relevant part, "the second decrypted information comprises game graphics and audio files." Similar to the discussion of claim 54, the cited references fails to describe this feature.

In addition, claim 37 recites, in relevant part, "the second decrypted information comprises new release game software files." Similar to the discussion of claim 55, the cited references do not teach or suggest this feature.

In addition, claim 39 recites, in relevant part, "wherein the third non-resident security key is packaged with the second encrypted electronic information into one file for transmission to the gaming terminal." Similar to the discussion of claim 57, the cited references do not teach or suggest this feature.

For at least the foregoing reasons, Applicant submits that Claims 23-30, 32-48 and 50-60 are allowable and respectfully request withdrawal the 35 U.S.C. § 103(a) rejection.

2. Rejection of claims 31 and 49 (35 U.S.C. § 102(e))

Claims 31 and 49 are rejected under 35 U.S.C. § 102(e), the Examiner contending they are anticipated by Alcorn in view of Hansmann and further in view of Elliot U.S. Patent No. 6,468,160 ("Elliot"). The Applicant notes that a 102(e) rejection may only be applied with a single reference. Based on the Office Action's discussion of an alleged motivation to combine, the Applicant has, for the purposes of this response, assumed the rejection is a 103(a) obviousness rejection.

Claim 31 depends from claim 23, and therefore includes all features recited in claim 23. Claim 49 depends from claim 43, and therefore includes all features recited in claim 43. As more fully set forth above, the combination of Alcorn and Hansmann does not disclose all of the features recited in claims 23 and 43. Elliot has not been asserted to overcome the shortcomings of Alcorn and Hansmann. As such, it is respectfully submitted that the combination of the cited references does not render unpatentable claims 31 and 49 for at least the reasons more fully set forth above in support of the patentability of claims 23 and 43.

3. Rejection of claims 61 and 62 (35 U.S.C. § 102(e))

Claims 61 and 62 are rejected under 35 U.S.C. § 102(e), the Examiner contending they are anticipated by Alcorn in view of Hansmann and further in view of Ahrens et al. U.S. Patent No. 6,018,695 ("Ahrens"). The Applicant notes that a 102(e) rejection may only be applied with a single reference. Based on the Office Action's discussion of an alleged motivation to combine, the Applicant has, for the purposes of this response, assumed the rejection is a 103(a) obviousness rejection.

Claim 61 depends from claim 23, and therefore includes all features recited in claim 23. Claim 62 depends from claim 43, and therefore includes all features recited in claim 43.

As more fully set forth above, the combination of Alcorn and Hansmann does not disclose all of the features recited in claims 23 and 43. Ahrens has not been asserted to overcome the shortcomings of Alcorn and Hansmann. As such, it is respectfully submitted that the combination of the cited references does not render unpatentable claims 61 and 62 for at least the reasons more fully set forth above in support of the patentability of claims 23 and 43.

Moreover, claim 62 recites decrypting the second encrypted electronic information into an interim result with the first resident security key at the gaming terminal, and decrypting the interim result into the second decrypted electronic information with the second non-resident security key at the gaming terminal." The Office Action admits that this feature is not found in either Hansmann or Alcorn. The proposed addition of Ahrens does not rectify the deficiencies of the combination. The recited claim feature addresses a particular way in which the first and second decryption keys may be used, i.e., one after the other, as opposed to, for example, simultaneously decrypting the data with the two keys combined. This feature is not taught or suggested in any of the cited references, and no such teaching is identified in the Office Action. Because this claim feature is not found in any of the cited references, the proposed combination does not render claim 62 obvious. Furthermore, the proposed motivation to combine "because a means to permit updating of software is needed", does not lead to the particular recited claim feature. The Office Action is entirely silent as to how the prior art would lead an ordinary artisan to employ the recited two-step decryption procedure. For at least this additional reason claim 62 is not obvious. Claim 61 should be allowable for similar reasons to claim 62.

4. New Claim 63

New claims 63 depends from claim 56, and therefore should be allowable for at least the same reasons as those given above for claim 56. Moreover, claim 63 expressly recites that the downloaded third key replaces the first resident key, a feature neither taught nor suggested by the cited references.

CONCLUSION

The Applicant respectfully submits that the present claims are in condition for allowance. Passage to issuance is, therefore, respectfully requested. All issues raised by the Examiner having been addressed, an early and favorable action on the merits is earnestly solicited.

The Office is authorized to charge any fees associated with this Amendment to Kenyon & Kenyon LLP Deposit Account No. 11-0600.

Respectfully Submitted,

KENYON & KENYON LLP

Dated: July 7, 2006

By: ______________

Andrew L. Reibman
(Reg. No. 47,893)

One Broadway
New York, NY 10004
(212) 425-7200

CUSTOMER NO. 26646